

What is claimed is:

1. A verification system for a computer software installation, comprising:

5 a primary library file, the primary library file having a digital signature;

a loader program arranged to obtain a digital signature key and further arranged to load the primary library file; and

10 a plurality of secondary files arranged to be referenced by the primary library file, each of the plurality of secondary files having a digital signature;

15 wherein the loader program is arranged to verify and selectively load the primary library file by comparing the obtained digital signature key with the digital signature of the primary library file, the primary library file being further arranged to subsequently verify and selectively load the plurality of secondary files by calling the loader program to compare the obtained digital signature key with the digital signature of each of the plurality of secondary files.

2. The verification system of claim 1, further characterised by:

25 the plurality of files including at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, wherein after successful

1005053-011002

verification and selective loading of the at least one secondary file, the at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file.

3. The verification system of claim 2, further characterised by:

the digital signature key being a public key obtained via the internet.

4. The verification system of claim 2, further characterised by:

the digital signature key being a hidden public key internal to the loader program, the loader program being arranged to use the hidden public key in the event that a public key cannot be obtained via the internet.

5. The verification system of claim 2, further characterised by:

the digital signature key comprising a number of keys including a private key provided by an administrator, wherein the plurality of files includes at least one administrator-configurable file, and

wherein the loader program is further arranged to verify the digital signature of the at least one administrator-configurable file using the private key.

6. The verification system of claim 5, further characterised by:

the software installation being a Java Virtual Machine installation.

7. A verification method for a computer software installation, the method comprising the steps of:

launching a loader program arranged to load files and further arranged to obtain a digital signature key;

using the loader program to verify the authenticity of a digital signature incorporated in a primary library file by comparing said digital signature with the digital signature key;

selectively loading the primary library file in dependence upon the successful verification of its digital signature;

using the primary library file and the loader program to verify the authenticity of digital signatures incorporated in each of the secondary files by comparing them with the digital signature key; and,

selectively loading the secondary files in dependence upon the successful verification of their digital signatures.

8. The verification method of claim 7, further characterised by:

the plurality of files including at least one tertiary file referenced by at least one secondary file of the plurality of secondary files,

the method comprising the further steps of:

after successful verification and selective loading of the at least one secondary files;

using the at least one secondary file to manage the verification and selective loading of the at least one tertiary file.

9. The verification method of claim 8, further characterised by:

the digital signature key being a public key obtained via the internet.

10. The verification method of claim 8, further characterised by:

the digital signature key being a hidden public key internal to the loader program, the loader program being arranged to use the hidden public key in the event that a public key cannot be obtained via the internet.

11. The verification method of claim 8, further characterised by:

the digital signature key comprising a number of keys including a private key provided by an administrator,

wherein the plurality of files includes at least one administrator-configurable file, and

wherein the loader program is further arranged to verify and selectively load the digital signature of the at least one administrator-configurable file using the private key.

12. The verification method of claim 8, further characterised by:

the software installation being a Java Virtual Machine installation.

13. A computer program element comprising computer program means for performing the method of claim 7.

5

10

10050083.011402